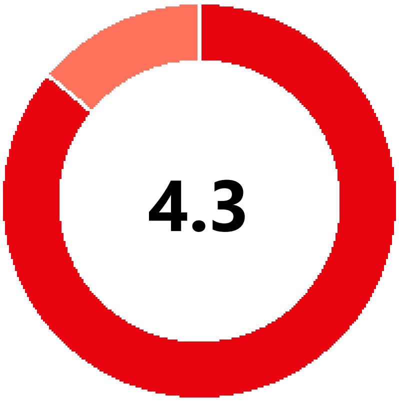
Target: **https://edistrict.kerala.gov.in**

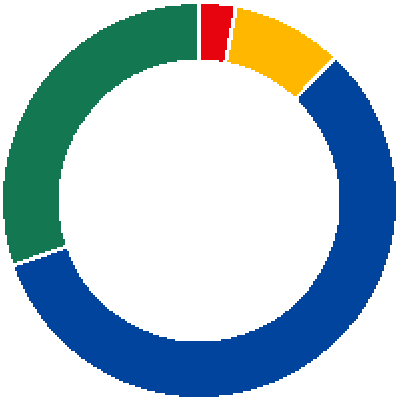
Date: **Tue Nov 29 2022**

Found Issues: **33**

scan **finished** within **12′ 2″** after **5621** requests.



Risk



Issue Severity

Executive Summary

SmartScanner conducted a scan on edistrict.kerala.gov.in to find security weaknesses and vulnerabilities. The scan took 12 minutes and 2 seconds. After performing 5621 requests, SmartScanner found 33 issues in which 1 of them is highly severe. The overall security risk of edistrict.kerala.gov.in is 4.3 out of 5. It is recommended to fix the found issues as soon as possible to mitigate the security risk. Technical details, as well as remediation of results, can be found in the following. *

* DISCLAIMER: This report is only limited to the results of SmartScanner findings.

List of Issues

1– Cross Site Scripting

1.1– https://edistrict.kerala.gov.in

2– Session Cookie without HttpOnly Flag

2.1– https://edistrict.kerala.gov.in

3– Session Cookie without SameSite Flag

3.1– https://edistrict.kerala.gov.in

4– Medium Impact Issue

4.1– https://edistrict.kerala.gov.in

5– BREACH attack

5.1– https://edistrict.kerala.gov.in/CivilCaseEvents.do?lang=%27%22%21%3F-%25s

5.2– https://edistrict.kerala.gov.in/edportalsignin.jsp#

5.3– https://edistrict.kerala.gov.in/findportalLoginname.do

5.4– https://edistrict.kerala.gov.in/generalService.htm?event=services&token=16696996094044164523144690436167

5.5– https://edistrict.kerala.gov.in/openSearch.do?openStat=openSearch&lang=en

5.6– https://edistrict.kerala.gov.in/portalPasswordReset.do

5.7– https://edistrict.kerala.gov.in/qrVerify.do?qr=qrVerify&lang=en

5.8– https://edistrict.kerala.gov.in/registerPortalUser.do

6– Auto Complete Enabled Password Input

6.1– https://edistrict.kerala.gov.in/edportalsignin.jsp

6.2– https://edistrict.kerala.gov.in/Login.htm

6.3– https://edistrict.kerala.gov.in/registerPortalUser.do

7– Strict-Transport-Security Header is Missing

7.1– https://edistrict.kerala.gov.in

8– Content-Security-Policy Header is Missing

8.1– https://edistrict.kerala.gov.in

9– X-Frame-Options Header is Missing

9.1– https://edistrict.kerala.gov.in

10– Cookie without HttpOnly Flag

10.1– https://edistrict.kerala.gov.in/registerPortalUser.do

11– Cookie without SameSite Flag

11.1– https://edistrict.kerala.gov.in/registerPortalUser.do

12– Cookie without Secure Flag

12.1– https://edistrict.kerala.gov.in/registerPortalUser.do

13– TRACE Method Allowed

13.1– https://edistrict.kerala.gov.in/

14– TLS 1.0 enabled

14.1– https://edistrict.kerala.gov.in

15– Broken Link

- 15.1– https://edistrict.kerala.gov.in/dwr/call/plaincall/__System.pageLoaded.dwr
- 15.2– https://edistrict.kerala.gov.in/Invalid.jsp

16– X-Content-Type-Options Header is Missing

- 16.1– https://edistrict.kerala.gov.in

17– Missing or Insecure Cache-Control Header

- 17.1– https://edistrict.kerala.gov.in/pubmenu.jsp

18– Cross-Origin Resource Sharing Allowed

- 18.1– https://edistrict.kerala.gov.in/registerPortalUser.do

19– Referrer-Policy Header is Missing

- 19.1– https://edistrict.kerala.gov.in

20– X-XSS-Protection Header is Set

- 20.1– https://edistrict.kerala.gov.in/registerPortalUser.do

21– Email Address Disclosure

- 21.1– https://edistrict.kerala.gov.in

22– Target Information

- 22.1– https://edistrict.kerala.gov.in

23– TLS 1.1 enabled

- 23.1– https://edistrict.kerala.gov.in

1.1 Cross Site Scripting

SEVERITY	High
URL	https://edistrict.kerala.gov.in

This type of issue is only available in the Professional version

2.1 Session Cookie without HttpOnly Flag

SEVERITY	Medium
URL	https://edistrict.kerala.gov.in
COOKIE	JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:46:39 GMT
Server: Apache
Set-Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8







<html lang="en">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" cont
...[truncated]...
```

DESCRIPTION

The `HttpOnly` cookie flag prevents JavaScript `Document.cookie` API from accessing the cookie. When this flag is set, the cookie is only sent to the server. In many cases, cookies are not needed on the client-side. Session cookies are a good example of cookies that don't need to be available to JavaScript. Using the `HttpOnly` flag can help to mitigate Cross-Site-Scripting(XSS) attacks.

RECOMMENDATION

Set `HttpOnly` flag for the cookie.

3.1 Session Cookie without SameSite Flag

SEVERITY	Medium
URL	https://edistrict.kerala.gov.in
COOKIE	JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:46:39 GMT
Server: Apache
Set-Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8







<html lang="en">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" cont
...[truncated]...
```

DESCRIPTION

The `SameSite` cookie flag with the right value prevents the browser from sending the cookie in cross-origin requests. It provides some protection against cross-site request forgery attacks (CSRF).

RECOMMENDATION

Set `SameSite` flag for the cookie.

4.1 Medium Impact Issue

SEVERITY	Medium
URL	https://edistrict.kerala.gov.in

This type of issue is only available in the Professional version

5.1 BREACH attack

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/CivilCaseEvents.do?lang=%27%22%21%3F-%25s

DETAILS

The value of query parameter `lang` is reflected in the response when HTTP compression was used. This can be used in a BREACH attack to find secrets in the response.

REQUEST / RESPONSE

#1

```
GET /CivilCaseEvents.do?lang=%27%22%21%3F-%25s HTTP/1.1
Content-Type: text/plain
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict
Referer:
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=65
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dt
d">
```

```
...[truncated]...
```

DESCRIPTION

BREACH is an instance of the CRIME attack against HTTP compression—the use of gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP by many web browsers and servers. Given this compression oracle, the rest of the BREACH attack follows the same general lines as the CRIME exploit, by performing an initial blind brute-force search to guess a few bytes, followed by divide-and-conquer search to expand a correct guess to an arbitrarily large amount of content. Wikipedia

RECOMMENDATION

Disable HTTP compression completely or at least on pages where a secret (like a session cookie) is being transferred. Disabling compression whenever the referrer header indicates a cross-site request, or when the header is not present is another suggested approach.
Generally, CSRF protection methods can be used as mitigation.

5.2 BREACH attack

SEVERITY Low

URL https://edistrict.kerala.gov.in/edportalsignin.jsp#

DETAILS

The value of post parameter `LangRadioGroup` is reflected in the response when HTTP compression was used. This can be used in a BREACH attack to find secrets in the response.

REQUEST / RESPONSE

#1

```
POST /edportalsignin.jsp HTTP/1.1
Referer: https://edistrict.kerala.gov.in/edportalsignin.jsp
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict;
Content-Length: 273

tknName=James%20Bond&token=16696996094044164523144690436167&j_password=DJrLcmno321@!&j_passwordhex=
DJrLcmno321@!&clientTime=&login=Test&j_username=Test&j_passwordtxt=DJrLcmno321@!&j_captcha_response
=&LangRadioGroup=English&LangRadioGroup=English&userType=Test&userType=Test
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:50:32 GMT
Server: Apache
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Pragma: no-cache
Cache-Control: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=66
Connection: Keep-Alive
Content-Type: text/html; UTF-8;charset=UTF-8





















<html lang="en" class="no-js">
<head>
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content=
...[truncated]...
```

DESCRIPTION

BREACH is an instance of the CRIME attack against HTTP compression—the use of gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP by many web browsers and servers. Given this compression oracle, the rest of the BREACH attack follows the same general lines as the CRIME exploit, by performing an initial blind brute-force search to guess a few bytes, followed by divide-and-conquer search to expand a correct guess to an arbitrarily large amount of content. Wikipedia

RECOMMENDATION

Disable HTTP compression completely or at least on pages where a secret (like a session cookie) is being transferred. Disabling compression whenever the referrer header indicates a cross-site request, or when the header is not present is another suggested approach.
Generally, CSRF protection methods can be used as mitigation.

5.3 BREACH attack

SEVERITY Low

URL https://edistrict.kerala.gov.in/findportalLoginname.do

DETAILS

The value of post parameter `Submit` is reflected in the response when HTTP compression was used. This can be used in a BREACH attack to find secrets in the response.

REQUEST / RESPONSE

#1

```
POST /findportalLoginname.do HTTP/1.1
Referer: https://edistrict.kerala.gov.in/findportalLoginname.do?token=16696996094044164523144690436
167
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=8fWXReDvgAhn+fx1Hr9YOQ__.node2; SameSite=strict;
Content-Length: 361

login=Test&tknName=James%20Bond&langVar=English&token=16696998357568978135314036777535&hidedpasswor
d=DJrLcmno321@!&hidemailid=test@none.nowhere.com&hidmobile=&hidusername=Test&hidloginname=Test&user
Name=Test&dob=&uid=&Submit=%20Submit&pageidentity=25&pass1=DJrLcmno321@!&cnfrmpass=DJrLcmno321@!&se
c_ques=&mobHidden=&hidPassword=DJrLcmno321@!&hidlogin=Test&phno=
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:54:08 GMT
Server: Apache
Set-Cookie: SameSite=strict;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=65
Connection: Keep-Alive
Content-Type: text/html; ;charset=UTF-8
```

```
<html lang="en">
<HEAD>
<script type='text/javascript' src='js/appValidate.js'></script>
<scrip
...[truncated]...
```

DESCRIPTION

BREACH is an instance of the CRIME attack against HTTP compression—the use of gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP by many web browsers and servers. Given this compression oracle, the rest of the BREACH attack follows the same general lines as the CRIME exploit, by performing an initial blind brute-force search to guess a few bytes, followed by divide-and-conquer search to expand a correct guess to an arbitrarily large amount of content. Wikipedia

RECOMMENDATION

Disable HTTP compression completely or at least on pages where a secret (like a session cookie) is being transferred. Disabling compression whenever the referrer header indicates a cross-site request, or when the header is not present is another suggested approach.
Generally, CSRF protection methods can be used as mitigation.

5.4 BREACH attack

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/generalService.htm?event=services&token=16696996094044164523144690436167

DETAILS

The value of query parameter `event` is reflected in the response when HTTP compression was used. This can be used in a BREACH attack to find secrets in the response.

REQUEST / RESPONSE

#1

```
GET /generalService.htm?event=services&token=16696996094044164523144690436167 HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=75
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8











<html lang='en'>
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name
...[truncated]...
```

DESCRIPTION

BREACH is an instance of the CRIME attack against HTTP compression—the use of gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP by many web browsers and servers. Given this compression oracle, the rest of the BREACH attack follows the same general lines as the CRIME exploit, by performing an initial blind brute-force search to guess a few bytes, followed by divide-and-conquer search to expand a correct guess to an arbitrarily large amount of content. Wikipedia

RECOMMENDATION

Disable HTTP compression completely or at least on pages where a secret (like a session cookie) is being transferred. Disabling compression whenever the referrer header indicates a cross-site request, or when the header is not present is another suggested approach.
Generally, CSRF protection methods can be used as mitigation.

5.5 BREACH attack

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/openSearch.do?openStat=openSearch&lang=en

DETAILS

The value of query parameter `openStat` is reflected in the response when HTTP compression was used. This can be used in a BREACH attack to find secrets in the response.

REQUEST / RESPONSE

#1

```
GET /openSearch.do?openStat=openSearch&lang=en HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=74
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">


















<html lang="en">
<head>
<meta charset="UTF
...[truncated]...
```

DESCRIPTION

BREACH is an instance of the CRIME attack against HTTP compression—the use of gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP by many web browsers and servers. Given this compression oracle, the rest of the BREACH attack follows the same general lines as the CRIME exploit, by performing an initial blind brute-force search to guess a few bytes, followed by divide-and-conquer search to expand a correct guess to an arbitrarily large amount of content. Wikipedia

RECOMMENDATION

Disable HTTP compression completely or at least on pages where a secret (like a session cookie) is being transferred. Disabling compression whenever the referrer header indicates a cross-site request, or when the header is not present is another suggested approach.
Generally, CSRF protection methods can be used as mitigation.

5.6 BREACH attack

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/portalPasswordReset.do

DETAILS

The value of post parameter `Submit` is reflected in the response when HTTP compression was used. This can be used in a BREACH attack to find secrets in the response.

REQUEST / RESPONSE

#1

```
POST /portalPasswordReset.do HTTP/1.1
Referer: https://edistrict.kerala.gov.in/portalPasswordReset.do?token=16696996094044164523144690436
167
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=8fWXReDvgAhn+fx1Hr9YOQ__.node2; SameSite=strict;
Content-Length: 416

login=Test&tknName=James%20Bond&langVar=English&token=16696998357578976482830820093407&login_name=T
est&login_go=Test&dob=&uid_no=&sec_ans=&Submit=%20Submit&newPass=DJrLcmno321@!&confirmPass=DJrLcmno
321@!&hidPassword1=DJrLcmno321@!&change=Submit&clearBtn=Clear&pageidentity=25&pass1=DJrLcmno321@!&c
nfrmpass=DJrLcmno321@!&sec_ques=&mobHidden=&hidPassword=DJrLcmno321@!&hidlogin=Test&ed_pswd=test@no
ne.nowhere.com&Go=Go
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:54:07 GMT
Server: Apache
Set-Cookie: SameSite=strict;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=67
Connection: Keep-Alive
Content-Type: text/html; ;charset=UTF-8
```

```
<html lang="en">

<HEAD>
<script type='text/javascript' src='js/appValidate.js'></script>
<scrip
...[truncated]...
```

DESCRIPTION

BREACH is an instance of the CRIME attack against HTTP compression—the use of gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP by many web browsers and servers. Given this compression oracle, the rest of the BREACH attack follows the same general lines as the CRIME exploit, by performing an initial blind brute-force search to guess a few bytes, followed by divide-and-conquer search to expand a correct guess to an arbitrarily large amount of content. Wikipedia

RECOMMENDATION

Disable HTTP compression completely or at least on pages where a secret (like a session cookie) is being transferred. Disabling compression whenever the referrer header indicates a cross-site request, or when the header is not present is another suggested approach.
Generally, CSRF protection methods can be used as mitigation.

5.7 BREACH attack

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/qrVerify.do?qr=qrVerify&lang=en

DETAILS

The value of query parameter `qr` is reflected in the response when HTTP compression was used. This can be used in a BREACH attack to find secrets in the response.

REQUEST / RESPONSE

#1

```
GET /qrVerify.do?qr=qrVerify&lang=en HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:32 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=64
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">



<html lang="en">
<head>

<meta http-equiv="
...[truncated]...
```

DESCRIPTION

BREACH is an instance of the CRIME attack against HTTP compression—the use of gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP by many web browsers and servers. Given this compression oracle, the rest of the BREACH attack follows the same general lines as the CRIME exploit, by performing an initial blind brute-force search to guess a few bytes, followed by divide-and-conquer search to expand a correct guess to an arbitrarily large amount of content. [Wikipedia]

RECOMMENDATION

Disable HTTP compression completely or at least on pages where a secret (like a session cookie) is being transferred. Disabling compression whenever the referrer header indicates a cross-site request, or when the header is not present is another suggested approach.
Generally, CSRF protection methods can be used as mitigation.

5.8 BREACH attack

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/registerPortalUser.do

DETAILS

The value of post parameter `otpemailid` is reflected in the response when HTTP compression was used. This can be used in a BREACH attack to find secrets in the response.

REQUEST / RESPONSE

#1

```
POST /registerPortalUser.do HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict
Referer:
Content-Length: 482

userName=Test&dobCalender=&gender=M&houseno_name=James%20Bond&place=&locality=&mobileNo=&uid=&login
Name=Test&login=Test&password=DJrLcmno321@!&confirmPassword=DJrLcmno321@!&hidPassword=DJrLcmno321@!
&passwordFlag=DJrLcmno321@!&securityAns=DJrLcmno321@!&j_captcha_response=&eventstr=&submitNewUser=T
est&submitNewUser=Test&otpid=test@none.nowhere.com&old_password=DJrLcmno321@!&change_password=DJrLc
mno321@!&scode=71983&districtCbo=-1&securityQnsCbo=-1&otpemailid=registerPortalUser.do
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:50:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=85
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dt
d
...[truncated]...
```

DESCRIPTION

BREACH is an instance of the CRIME attack against HTTP compression—the use of gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP by many web browsers and servers. Given this compression oracle, the rest of the BREACH attack follows the same general lines as the CRIME exploit, by performing an initial blind brute-force search to guess a few bytes, followed by divide-and-conquer search to expand a correct guess to an arbitrarily large amount of content. Wikipedia

RECOMMENDATION

Disable HTTP compression completely or at least on pages where a secret (like a session cookie) is being transferred. Disabling compression whenever the referrer header indicates a cross-site request, or when the header is not present is another suggested approach.
Generally, CSRF protection methods can be used as mitigation.

6.1 Auto Complete Enabled Password Input

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/edportalsignin.jsp

REQUEST / RESPONSE

#1

```
GET /edportalsignin.jsp HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:14 GMT
Server: Apache
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Pragma: no-cache
Cache-Control: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; UTF-8;charset=UTF-8



















<html lang="en" class="no-js">
<head>
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/ht
...[truncated]...
```

DESCRIPTION

The user browser can save and remember the entered values for user input fields with autocomplete enabled attributes. This might reveal sensitive information like passwords, especially in public and multi-user computers.

RECOMMENDATION

Add the attribute `autocomplete="off"` for sensitive form inputs.

6.2 Auto Complete Enabled Password Input

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/Login.htm

REQUEST / RESPONSE

#1

```
POST /Login.htm HTTP/1.1
Referer: https://edistrict.kerala.gov.in/edportalsignin.jsp
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict;
Content-Length: 180

tknName=James%20Bond&token=16696996094044164523144690436167&userId=Test&slno=&subject=&issue=&certi
ficate=&notBefore=&notAfter=&login=Test&edencsignature=&edenckey=&encdata=&alias=
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:50:32 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; UTF-8;charset=UTF-8



<html lang="en" class="no-js">
<head>
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content=
...[truncated]...
```

DESCRIPTION

The user browser can save and remember the entered values for user input fields with autocomplete enabled attributes. This might reveal sensitive information like passwords, especially in public and multi-user computers.

RECOMMENDATION

Add the attribute `autocomplete="off"` for sensitive form inputs.

6.3 Auto Complete Enabled Password Input

SEVERITY Low

URL https://edistrict.kerala.gov.in/registerPortalUser.do

REQUEST / RESPONSE

#1

```
GET /registerPortalUser.do HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8






















<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dt
d">



...[truncated]...
```

DESCRIPTION

The user browser can save and remember the entered values for user input fields with autocomplete enabled attributes. This might reveal sensitive information like passwords, especially in public and multi-user computers.

RECOMMENDATION

Add the attribute `autocomplete="off"` for sensitive form inputs.

7.1 Strict-Transport-Security Header is Missing

SEVERITY	Low
URL	https://edistrict.kerala.gov.in
AFFECTED URLS (19)	edistrict.kerala.gov.in/Login.htm edistrict.kerala.gov.in/registerPortalUser.do edistrict.kerala.gov.in/edportalsignin.jsp edistrict.kerala.gov.in/pubmenu.jsp edistrict.kerala.gov.in/Invalid.jsp edistrict.kerala.gov.in/dwr/call/plaincall/__System.generateId.dwr edistrict.kerala.gov.in/dwr/call/plaincall/__System.pageLoaded.dwr edistrict.kerala.gov.in/generalService.htm edistrict.kerala.gov.in/governmentOrders.jsp edistrict.kerala.gov.in/captcha.do edistrict.kerala.gov.in/portalPasswordReset.do edistrict.kerala.gov.in/findportalLoginname.do edistrict.kerala.gov.in edistrict.kerala.gov.in/CivilCaseEvents.do edistrict.kerala.gov.in/portalfooter.jsp edistrict.kerala.gov.in/dwr/call/plaincall/loginDAO.getserverDate.dwr edistrict.kerala.gov.in/openSearch.do edistrict.kerala.gov.in/qrVerify.do edistrict.kerala.gov.in/officialPasswordReset.do

REQUEST / RESPONSE

1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:46:39 GMT
Server: Apache
Set-Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8







<html lang="en">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" cont
...[truncated]...
```

DESCRIPTION

The HTTP Strict-Transport-Security response header (often abbreviated as HSTS) lets a web site tell browsers that it should only be accessed using HTTPS, instead of using HTTP. Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

8.1 Content-Security-Policy Header is Missing

SEVERITY	Low
URL	https://edistrict.kerala.gov.in
AFFECTED URLS (15)	edistrict.kerala.gov.in/portalPasswordReset.do edistrict.kerala.gov.in/qrVerify.do edistrict.kerala.gov.in/officialPasswordReset.do edistrict.kerala.gov.in/pubmenu.jsp edistrict.kerala.gov.in edistrict.kerala.gov.in/findportalLoginname.do edistrict.kerala.gov.in/Login.htm edistrict.kerala.gov.in/openSearch.do edistrict.kerala.gov.in/generalService.htm edistrict.kerala.gov.in/registerPortalUser.do edistrict.kerala.gov.in/Invalid.jsp edistrict.kerala.gov.in/edportalsignin.jsp edistrict.kerala.gov.in/CivilCaseEvents.do edistrict.kerala.gov.in/governmentOrders.jsp edistrict.kerala.gov.in/portalfooter.jsp

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:46:39 GMT
Server: Apache
Set-Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8








<html lang="en">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" cont
...[truncated]...
```

DESCRIPTION

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware. Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

9.1 X-Frame-Options Header is Missing

SEVERITY	Low
URL	https://edistrict.kerala.gov.in
AFFECTED URLS (6)	edistrict.kerala.gov.in/pubmenu.jsp edistrict.kerala.gov.in edistrict.kerala.gov.in/Invalid.jsp edistrict.kerala.gov.in/edportalsignin.jsp edistrict.kerala.gov.in/governmentOrders.jsp edistrict.kerala.gov.in/portalfooter.jsp

REQUEST / RESPONSE

1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:46:39 GMT
Server: Apache
Set-Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8







<html lang="en">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" cont
...[truncated]...
```

DESCRIPTION

The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a `<frame>`, `<iframe>`, `<embed>` or `<object>`. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites.
Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

10.1 Cookie without HttpOnly Flag

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/registerPortalUser.do
COOKIE	SameSite=strict

REQUEST / RESPONSE

#1

```
GET /registerPortalUser.do HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8




<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">


...[truncated]...
```

DESCRIPTION

The `HttpOnly` cookie flag prevents JavaScript `Document.cookie` API from accessing the cookie. When this flag is set, the cookie is only sent to the server. In many cases, cookies are not needed on the client-side. Session cookies are a good example of cookies that don’t need to be available to JavaScript. Using the `HttpOnly` flag can help to mitigate Cross-Site-Scripting(XSS) attacks.

RECOMMENDATION

Set `HttpOnly` flag for the cookie.

11.1 Cookie without SameSite Flag

SEVERITY	Low
URL	https://edistrict.kerala.gov.in/registerPortalUser.do
COOKIE	SameSite=strict

REQUEST / RESPONSE

#1

```
GET /registerPortalUser.do HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8



<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dt
d">


...[truncated]...
```

DESCRIPTION

The `SameSite` cookie flag with the right value prevents the browser from sending the cookie in cross-origin requests. It provides some protection against cross-site request forgery attacks (CSRF).

RECOMMENDATION

Set `SameSite` flag for the cookie.

12.1 Cookie without Secure Flag

SEVERITY Low

URL https://edistrict.kerala.gov.in/registerPortalUser.do

COOKIE SameSite=strict

REQUEST / RESPONSE

#1

```
GET /registerPortalUser.do HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8




<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dt
d">


...[truncated]...
```

DESCRIPTION

The `Secure` cookie flag prevents the browser from sending the cookie over an unencrypted connection. A cookie with a `Secure` flag is sent to the server only with an encrypted request over the HTTPS protocol. Therefore it can’t easily be accessed by a man-in-the-middle attacker.

RECOMMENDATION

Set `Secure` flag for the cookie.

13.1 TRACE Method Allowed

SEVERITY Low

URL https://edistrict.kerala.gov.in/

REQUEST / RESPONSE

#1

```
TRACE / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:25 GMT
Server: Apache
Keep-Alive: timeout=5, max=77
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

TRACE / HTTP/1.1
Host: edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xh
...[truncated]...
```

DESCRIPTION

HTTP TRACE method allows a client to see the whole request that the webserver has received. The main purpose of this feature is for testing or diagnostic information.
This method can reveal sensitive information like Cookies and Authorization tokens to clients when they’re not supposed to access these data. This is often called a **Cross-Site Tracing (XST)** attack.

RECOMMENDATION

Disable the TRACE method in the webserver configuration.
For the Apache web server, add the below line to the main configuration file.

```
TraceEnable off
```

For Microsoft IIS open **ISS Manager**, go to **Request Filtering**, and change the configuration for TRACK and TRACE verbs in **HTTP Verbs**.

14.1 TLS 1.0 enabled

SEVERITY	Low
URL	https://edistrict.kerala.gov.in

DESCRIPTION

TLS version 1.0 has several flaws and is considered vulnerable.

RECOMMENDATION

Disable TLS 1.0 and replace it with TLS 1.2 or 1.3 protocols.

15.1 Broken Link

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in/dwr/call/plaincall/__System.pageLoaded.dwr
REFERER	https://edistrict.kerala.gov.in

REQUEST / RESPONSE

1

```
POST /dwr/call/plaincall/__System.pageLoaded.dwr HTTP/1.1
Referer: https://edistrict.kerala.gov.in
Content-Type: text/plain
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict;
Content-Length: 174

callCount=1
windowName=
c0-scriptName=__System
c0-methodName=pageLoaded
c0-id=0
batchId=0
instanceId=0
page=%2F
scriptSessionId=wCPvCPWdIe7TVjErviGuQazS2jo/grDS2jo-vzUd4fGR7
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:16 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Content-Type: text/javascript;charset=utf-8

throw 'allowScriptTagRemoting is false.';
(function(){
var r=window.dwr._[0];
//#DWR-INSERT
//#DWR-REPLY
r.handleCallback("0","0",null);
})();
```

DESCRIPTION

Broken hyperlinks in web pages can create a bad experience for the users. It can also affect the web page ranking in web search results.

RECOMMENDATION

Consider removing or fixing the link.

15.2 Broken Link

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in/Invalid.jsp
REFERER	https://edistrict.kerala.gov.in/Login.htm

REQUEST / RESPONSE

#1

```
GET /Invalid.jsp HTTP/1.1
Referer: https://edistrict.kerala.gov.in/Login.htm
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=5ZXmhzWhmkNGxsTwpAR-3w__.node2; SameSite=strict;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:53:47 GMT
Server: Apache
Set-Cookie: JSESSIONID=66vL+d3WKYL26iRAzjKp9g__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=ISO-8859-1


<html>
<head>
<style>
a:link                  {
        font:10pt/12pt verdana;
        color:#6666FF;
        text-decoration: none;
        font-weight:bold;
}
a:visited               {
        font:10pt/12pt
...[truncated]...
```

DESCRIPTION

Broken hyperlinks in web pages can create a bad experience for the users. It can also affect the web page ranking in web search results.

RECOMMENDATION

Consider removing or fixing the link.

16.1 X-Content-Type-Options Header is Missing

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in
AFFECTED URLS (9)	edistrict.kerala.gov.in/dwr/call/plaincall/loginDAO.getserverDate.dwr edistrict.kerala.gov.in/dwr/call/plaincall/__System.pageLoaded.dwr edistrict.kerala.gov.in/pubmenu.jsp edistrict.kerala.gov.in edistrict.kerala.gov.in/dwr/call/plaincall/__System.generateId.dwr edistrict.kerala.gov.in/Invalid.jsp edistrict.kerala.gov.in/edportalsignin.jsp edistrict.kerala.gov.in/governmentOrders.jsp edistrict.kerala.gov.in/portalfooter.jsp

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:46:39 GMT
Server: Apache
Set-Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8







<html lang="en">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" cont
...[truncated]...
```

DESCRIPTION

The `X-Content-Type-Options` response HTTP header is used by the server to prevent browsers from guessing the media type (MIME type).
This is known as **MIME sniffing** in which the browser guesses the correct MIME type by looking at the contents of the resource.
The absence of this header might cause browsers to transform non-executable content into executable content.

RECOMMENDATION

Configure your server to send this header with the value set to `nosniff`.

17.1 Missing or Insecure Cache-Control Header

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in/pubmenu.jsp

DETAILS

The `Cache-Control` header is not set

REQUEST / RESPONSE

#1

```
GET /pubmenu.jsp HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://edistrict.kerala.gov.in/registerPortalUser.do
Accept: text/html, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; SameSite=strict;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:50:31 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=67
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8



        <title>e D i s t r i c t Kerala</title>

   <link rel="stylesheet" href="css/custom.css">
   <link rel="stylesheet" href="css/fontawesome-free/css/all
...[truncated]...
```

DESCRIPTION

Web cache or HTTP cache is a system for optimizing the web. Browsers cache contents of a resource once and reuse it on consequent requests. Caching images on the web can boost page load time. But clients should not be allowed to cache pages that display sensitive, dynamic, or user specific contents.

RECOMMENDATION

Set any of following headers to prevent clients from caching the page.

```
Cache-Control: no-cache, no-store
```

```
Cache-Control: max-age=0, must-revalidate
```

```
Cache-Control: private
```

18.1 Cross-Origin Resource Sharing Allowed

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in/registerPortalUser.do
AFFECTED URLS (10)	edistrict.kerala.gov.in/captcha.do edistrict.kerala.gov.in/portalPasswordReset.do edistrict.kerala.gov.in/qrVerify.do edistrict.kerala.gov.in/officialPasswordReset.do edistrict.kerala.gov.in/findportalLoginname.do edistrict.kerala.gov.in/Login.htm edistrict.kerala.gov.in/openSearch.do edistrict.kerala.gov.in/generalService.htm edistrict.kerala.gov.in/registerPortalUser.do edistrict.kerala.gov.in/CivilCaseEvents.do

REQUEST / RESPONSE

#1

```
GET /registerPortalUser.do HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

```



<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">



...[truncated]...
```

DESCRIPTION

Cross-Origin Resource Sharing (CORS) is a mechanism that uses additional HTTP headers to tell browsers to give a web application running at one origin, access to selected resources from a different origin. A web application executes a cross-origin HTTP request when it requests a resource that has a different origin (domain, protocol, or port) from its own. Mozilla
Cross-origin resource sharing should not be allowed unless specifically needed to minimize disclosure of sensitive information to foreign origins.

RECOMMENDATION

Consider removing the `Access-Control-Allow-Origin` header or use specific origins as value.

19.1 Referrer-Policy Header is Missing

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in
AFFECTED URLS (15)	edistrict.kerala.gov.in/portalPasswordReset.do edistrict.kerala.gov.in/qrVerify.do edistrict.kerala.gov.in/officialPasswordReset.do edistrict.kerala.gov.in/pubmenu.jsp edistrict.kerala.gov.in edistrict.kerala.gov.in/findportalLoginname.do edistrict.kerala.gov.in/Login.htm edistrict.kerala.gov.in/openSearch.do edistrict.kerala.gov.in/generalService.htm edistrict.kerala.gov.in/registerPortalUser.do edistrict.kerala.gov.in/Invalid.jsp edistrict.kerala.gov.in/edportalsignin.jsp edistrict.kerala.gov.in/CivilCaseEvents.do edistrict.kerala.gov.in/governmentOrders.jsp edistrict.kerala.gov.in/portalfooter.jsp

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:46:39 GMT
Server: Apache
Set-Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8







<html lang="en">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" cont
...[truncated]...
```

DESCRIPTION

The `Referrer-Policy` HTTP header controls how much referrer information (sent via the `Referer` header) should be included with requests. Mozilla

The `Referer` (sic) header contains the address of the previous web page from which a link to the currently requested page was followed, which has lots of fairly innocent uses including analytics, logging, or optimized caching. However, there are more problematic uses such as tracking or stealing information, or even just side effects such as inadvertently leaking sensitive information. Mozilla

RECOMMENDATION

Configure your server to send the `Referrer-Policy` header for all pages with the value set to `strict-origin-when-cross-origin`. You can see references for other possible values.

20.1 X-XSS-Protection Header is Set

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in/registerPortalUser.do
AFFECTED URLS (9)	edistrict.kerala.gov.in/portalPasswordReset.do edistrict.kerala.gov.in/qrVerify.do edistrict.kerala.gov.in/officialPasswordReset.do edistrict.kerala.gov.in/findportalLoginname.do edistrict.kerala.gov.in/Login.htm edistrict.kerala.gov.in/openSearch.do edistrict.kerala.gov.in/generalService.htm edistrict.kerala.gov.in/registerPortalUser.do edistrict.kerala.gov.in/CivilCaseEvents.do

REQUEST / RESPONSE

#1

```
GET /registerPortalUser.do HTTP/1.1
Referer: https://edistrict.kerala.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2;
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:47:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: gzip
Access-Control-Allow-Origin: *
Set-Cookie: SameSite=strict;
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

```


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">



...[truncated]...
```

DESCRIPTION

The HTTP `X-XSS-Protection` response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Mozilla

- Chrome has removed their XSS Auditor
- Firefox has not, and will not implement X-XSS-Protection
- Edge has retired their XSS filter

> This means that if you do not need to support legacy browsers, it is recommended that you use `Content-Security-Policy` without allowing `unsafe-inline` scripts instead.

RECOMMENDATION

Do not send this header or set `0` as value.

21.1 Email Address Disclosure

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in
FOUND EMAILS	edistrict.ksitm@kerala.gov.in
FOUND IN (96)	edistrict.kerala.gov.in/generalService.htm?event=services and 1%3E0&token=16696996094044164523144690436167 edistrict.kerala.gov.in/generalService.htm?event=services%27%3B if %281%3D1%29 waitfor delay %2700%3A00%3A13%27--&token=16696996094044164523144690436167 edistrict.kerala.gov.in/qrVerify.do?lang=en&qr=qrVerify edistrict.kerala.gov.in/qrVerify.do?lang=99999%27 or 1%3E0-- a&qr=qrVerify edistrict.kerala.gov.in/generalService.htm?event=services and 1%3E1&token=16696996094044164523144690436167 edistrict.kerala.gov.in/generalService.htm?event=services%3B if %281%3D1%29 waitfor delay %2700%3A00%3A13%27--&token=16696996094044164523144690436167 edistrict.kerala.gov.in/qrVerify.do?lang=en&qr=qrVerify%3B if %281%3D1%29 waitfor delay %2700%3A00%3A13%27-- edistrict.kerala.gov.in/qrVerify.do?lang=en%3B if %281%3D1%29 waitfor delay %2700%3A00%3A13%27--&qr=qrVerify edistrict.kerala.gov.in/qrVerify.do?lang=en&qr%5B%5D= edistrict.kerala.gov.in/qrVerify.do?qr=qrVerify edistrict.kerala.gov.in/qrVerify.do?lang=en&qr=qrVerify rlike %28case when 1 then BENCHMARK%281862100000%2CMD5%280x41%29%29 else 0 end%29 -- a edistrict.kerala.gov.in/generalService.htm?event=services%27 and %271%27%3E%271&token=16696996094044164523144690436167 edistrict.kerala.gov.in/qrVerify.do?lang=en%27 and 1%3E1-- a&qr=qrVerify edistrict.kerala.gov.in/generalService.htm?event=99999 or 1%3E0&token=16696996094044164523144690436167 edistrict.kerala.gov.in/generalService.htm?event=services rlike %28case when 1 then BENCHMARK%281861500000%2CMD5%280x41%29%29 else 0 end%29 -- a&token=16696996094044164523144690436167 edistrict.kerala.gov.in/governmentOrders.jsp?lang%5B%5D= edistrict.kerala.gov.in/qrVerify.do?lang=en&qr=a%7Cid edistrict.kerala.gov.in/generalService.htm?event=a%26ping 2130706433%26%23%27%26ping 2130706434%26a%26%23%22%26ping 2130706435%26a%5C&token=16696996094044164523144690436167 edistrict.kerala.gov.in/generalService.htm?event=example.com%2F%3F&token=16696996094044164523144690436167 edistrict.kerala.gov.in/governmentOrders.jsp?lang=en%27%3B if %281%3D1%29 waitfor delay %2700%3A00%3A13%27-- ...

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 04:46:39 GMT
Server: Apache
Set-Cookie: JSESSIONID=ctpMI8wB9hrM3K6E3iAujQ__.node2; Path=/; Secure
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

...[truncated]...
   >Cancellation and Refund-Policy</a></li>


...[truncated]...
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

22.1 Target Information

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in
COOKIES	JSESSIONID SameSite
EMAILS	edistrict.ksitm@kerala.gov.in
FORMS WITH PASSWORD	https://edistrict.kerala.gov.in/Login.htm https://edistrict.kerala.gov.in/portalPasswordReset.do?token=166969960940441645231446904361 67 https://edistrict.kerala.gov.in/edportalsignin.jsp https://edistrict.kerala.gov.in/officialPasswordReset.do?token=166969960940441645231446904361 67 https://edistrict.kerala.gov.in/registerPortalUser.do
HTTPS	TLS 1.1 TLS 1.2 Heartbeat Extention TLS 1.0
SERVER BANNER	apache
SERVICES	HTTPS
WEB SERVER	apache

23.1 TLS 1.1 enabled

SEVERITY	Informational
URL	https://edistrict.kerala.gov.in

DESCRIPTION

TLS version 1.1 has several flaws and is considered not secure.

RECOMMENDATION

Disable TLS 1.1 and replace it with TLS 1.2 or 1.3 protocols.